PREPARING FOR FUTURE ATTACKS

SOLUTION BRIEF: IMPLEMENTING THE RIGHT SECURITY STRATEGY NOW

INTRODUCTION

Recent malware incidents have shown how costly and damaging cyber attacks can be.

The Stuxnet worm is believed to have significantly affected Iranian nuclear processing, and was widely considered to be the first operational cyber weapon[1]. Shamoon was able to compromise and incapacitate 30,000 work stations within an oil producing organisation[2]. Another targeted malware attack against a public corporation resulted in the company declaring a $66 million loss relating to the attack[3].

Such attacks may not necessarily be successful, but when attackers do find their way inside an organisation's systems, a swift, well-prepared response can quickly minimise damage and restore systems before significant harm can be caused.

In order to prepare such a response, organisations must understand how attacks can progress, develop a counteractive strategy, decide who will carry out which actions and then practise and refine the plan.

UNDERSTANDING ATTACKS

An attack starts with a point of ingress to the organisation. This may be an unsecured system that hackers are able to access, a vulnerable machine on which malware is executed, or a user who has been duped into installing malware. This point of ingress may then be exploited to spread attacks through the network, either by hacking other systems or by using malware to exploit unpatched system vulnerabilities and install itself on other systems.

Once a system is compromised, attackers may install further malware, or take control of the system and send commands for execution. Attackers may seek to exfiltrate information such as confidential files or usernames and passwords held on the system.

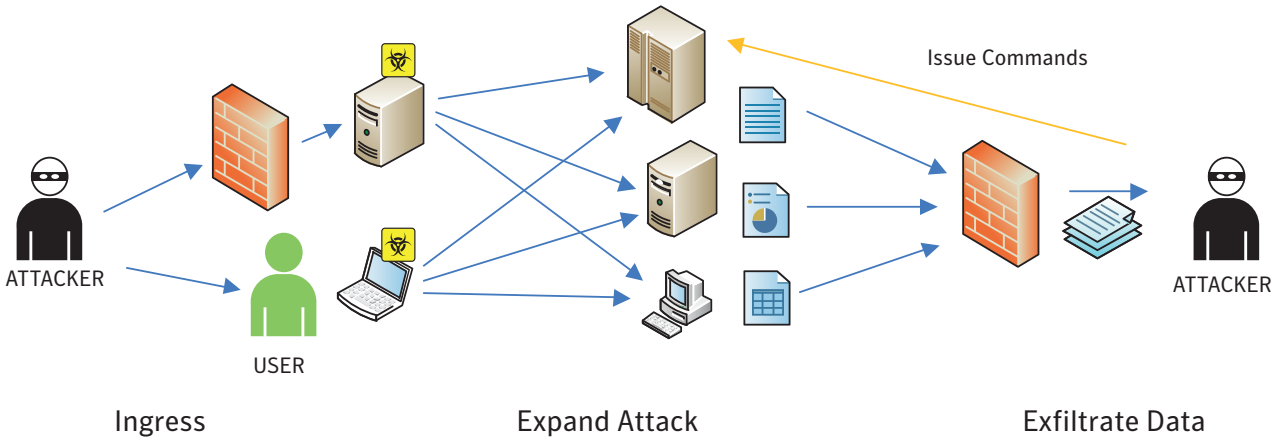


Figure 1: Schema of attack progression

PROTECTING AGAINST ATTACKS

Most attacks can be defended against with the implementation of basic information security practices. The Australian Department of Defence found that implementing four mitigation strategies was sufficient to prevent 85% of targeted attacks[4]. The British Government has advised that focusing on ten key areas is sufficient to counteract most cyber threats[5].

As a minimum, an organisation should ensure that network traffic and systems are scanned for malware and that logs of system and network activity are kept, to be used for forensic analysis if necessary. Additionally, regular backups are vital to ensure that damaged systems can be restored to a normal working state.

Adequate information security defences reduce the likelihood of attacks succeeding. However, behind every cyber attack headline is an organisation that believed its defences were sufficient. Major incidents do occur and need to be planned for, in order to reduce disruption to the business, minimise harm and reduce the time required for recovery.

PREPARING FOR INCIDENTS

Organisations should expect sophisticated attacks to be launched against their systems and prepare for this eventuality accordingly. In practice, such attacks are rare. However, by keeping abreast of the latest attacks and attacker techniques, organisations can verify that their systems are capable of detecting and repelling such threats.

Attention to the preparation process ensures that when an attack occurs, it is rapidly detected. Many identified incidents may be, on closer analysis, false positives, and many will be minor and will not require a major response. Nevertheless, organisations should be sure that they are capturing and recording all incidents so that the attacks that do require attention are quickly identified and escalated. To do this, it is important to determine the escalation criterion and mechanism by which a detected incident will activate an incident plan.

The first step of the incident plan should be an assessment of the situation. This should be followed by actions to prevent the attack from spreading to affect more systems and to prevent further harm from being incurred. Systems that have been infected will need isolating to contain the attack. Systems as yet uninfected may need to be temporarily disabled to prevent the attack from spreading internally, and network access may need to be curtailed.

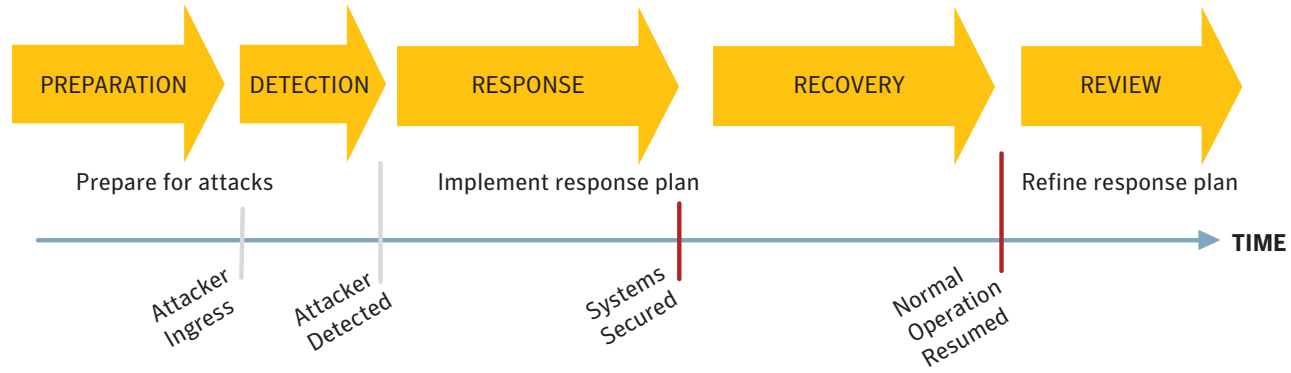


Figure 2: Incidence response phases

These actions may impact on users and services throughout the organisation. Notably, they may effect how users, and indeed the response team, usually communicate. Therefore, consideration needs to be given to how communication will be maintained and how users and executives will be kept up-to-date with the progress of incident resolution.

Forensic analysis should be used, not only to help identify if data has been compromised, but also to assess how attackers initially penetrated the systems. The vulnerability that was exploited to gain access needs to be addressed as a priority to prevent the attack being repeated as soon as it has been resolved. The collection and preservation of forensic information may also help in identifying and prosecuting those responsible for the attack.

The recovery phase involves restoring systems to their pre-infection state. Access to recent backups of the affected systems can greatly facilitate this process, providing they are free from malware. Care must be taken to ensure that systems are restored to an infection-free state.

Each incident should be subsequently reviewed to identify which procedures worked well, and where existing practices were lacking. The opportunity should be taken to learn from the incident and improve procedures in order to increase the security posture of the organisation.

CREATING A RESPONSE TEAM

Every organisation needs not only a response plan, but also a team who will implement it. So, a key factor for success will be the support of senior management. Indeed, when an incident is evolving fast, the involvement of a senior manager with the authority to approve whatever measures are necessary to contain and resolve the incident may be vital for gaining a speed advantage over the attackers.

Relevant stakeholders from departments that may be affected by an incident will need to be included as part of the response team. However, the greatest input to the team will be from the technical staff, who will implement the plan and possess the skills to remediate damage.

Organisations shouldn't feel that every position in the response team needs to be filled by in-house staff. External expertise should be considered for the specialist skills, and experience with similar incidents, that can be brought to the team.

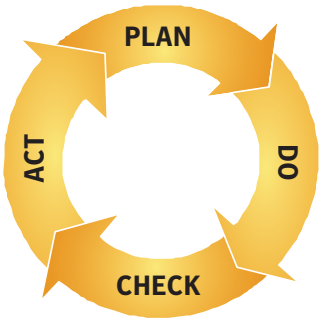
The composition of the team also needs to be regularly reviewed. Members may be required to be on-call for extended periods of time and might benefit from being rotated out of the incident team in order to rest. Equally, exercises and testing could identify additional skills that need to be brought into the team.

TESTING THE PLAN

Major attacks are rare events. The ideal outcome is that the incident plan and the skills of the response team will never need to be put into action. However, this brings risks of its own. Regularly testing the incident plan will reveal areas of weakness and prevent skills from being forgotten through lack of use.

Testing exercises may be paper-based, where the response to an evolving attack and resolution of the incident is played out on a theoretical basis. Or, such testing may be scheduled as a live exercise involving a team of penetration testers that simulate how attackers may compromise systems.

Regular exercises ensure that team members are comfortable with their roles and responsibilities. Testing a variety of different attack scenarios ensures that procedures are both comprehensive and flexible enough to respond to future attacks. Teams should adopt the model of: plan, do, check and act.



PLAN	Establish objectives, policies and procedures to meet the requirements of the business.
DO	Implement these policies and procedures.
CHECK	Verify if these are effective at meeting objectives in practice.
ACT	Take action to modify plans according to experience gained to refine and improve.

MORE FOCUS, LESS RISK.

CONCLUSION

Understanding how attacks can occur, implementing the right procedures and developing a clear response strategy can help organisations to counteract future threats and recover from incidents more quickly.

REFERENCES

1 N. Falliere, L. O. Murchu, E. Chien, "W32. Stuxnet Dossier", Symantec Security Response Whitepaper, February 2007
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
S. Davies, "Out of Control", Engineering & Technology v.6 (6) p.60-62, July 2011

2 D. Walker "Saudi Oil Company Back Online After Cyber Sabotage Attempt", SC Magazine, 27 Aug 2012
http://www.scmagazine.com/saudi-oil-company-back-online-after-cyber-sabotage-attempt/article/256313/

3 H. Tsukayama, "Cyber Attack on RSA Cost EMC $66 Million", The Washington Post, 26 Jul 2011
http://www.washingtonpost.com/blogs/post-tech/post/cyber-attack-on-rsa-cost-emc-66-million/2011/07/26/gIQA1ceKbI_blog.html

4 "Top Four Mitigation Strategies to Protect Your ICT System", Australian Government Department of Defence Intelligence and Security, p. 1, September 2011
http://www.dsd.gov.au/publications/Top_4_Mitigation_Strategies_to_Protect_Your_ICT_System.pdf

5 "Executive Companion: 10 Steps to Cyber Security", Dept. for Business Innovation & Skills, Centre for the Protection of National Infrastructure, Office of Cyber Security & Information Assurance, p. 1, September 2012
http://www.bis.gov.uk/assets/biscore/business-sectors/docs/0-9/12-1120-10-steps-to-cyber-security-executive.pdf

MORE FOCUS, LESS RISK.

Symantec

FURTHER READING

"Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology", NIST SP 800-61 rev. 2.
http://csrc.nist.gov/publications/nistpubs/800-61rev2/SP800-61rev2.pdf

"Guide to Malware Incident Prevention and Handling. Recommendations of the National Institute of Standards and Technology", NIST SP 800-83.
http://csrc.nist.gov/publications/nistpubs/800-83/SP800-83.pdf

BS ISO/IEC 27002:2005 Information technology
– Security techniques – Code of practice for information security management.

BS ISO/IEC 27035:2011 Information technology – Security techniques – Information security incident management.

PD ISO/IEC TR 18044:2004 Information technology – Security techniques – Information security incident management.

BS ISO/IEC 27031:2011 Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity.

"Best Practices for Troubleshooting Viruses on a Network", Symantec Knowledge Base. http://www.symantec.com/docs/TECH122466

B. Nahorney & E. Maengkom, "Containing an Outbreak.
How to clean your network after an incident.", Symantec Security Response Whitepaper.
http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/containing_an_outbreak.pdf

Symantec Security Response, "Security Best Practices"
http://www.symantec.com/theme.jsp?themeid=stopping_malware

Symantec Training, "Security Awareness Program"
http://www.symantec.com/products-solutions/training/theme.jsp?themeid=ssap

Solution Brief: Symantec Managed Security Services, "Symantec Security Monitoring Services: Security log management, monitoring, and analysis by certified experts"
http://www.symantec.com/content/en/us/enterprise/fact_sheets/b-security_monitoring_services_21042033.en-us.pdf

Solution Brief: Symantec Managed Security Services, "Symantec Managed Protection Services: Optimize enterprise security protection while maintaining control"
http://www.symantec.com/content/en/us/enterprise/fact_sheets/b-managed_protection_services_21042032.en-us.pdf

RECOMMENDATIONS

http://www.symantec.com/products-solutions/training/theme.jsp?themeid=ssap
http://www.symantec.com/products-solutions/training/training-paths/path.jsp?pathID=cloud_security_solution

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Symantec is a global leader in providing security, storage and systems management solutions to help customers secure and manage their information and identities.